REMARKS

In the Office Action dated July 28, 2008, claims 20-26 were objected to because the Examiner considered beginning each of the dependent claims with the phrase "A method as claimed in claim 1..." to be an "informality." Apparently, the Examiner believes that the proper beginning for a dependent claim should be "The method of claim 1 further comprising." If this is the basis for the Examiner's rejection, Applicant respectfully disagrees. The manner by which a dependent claim begins is purely a stylistic preference, and several of the references of record in the present prosecution begin each dependent claim in the same manner as the claims of the present application, or in a very similar manner. Whether each dependent claim begins with the word "A" or the word "The" is purely a stylistic preference, and there is no statutory requirement that governs such language.

Moreover, although in some instances the term "further comprising" may be useful, the use of that phrase in every dependent claim serves no purpose, and does not provide any additional clarification, since the transition word "comprising" is already open-ended, by definition, and therefore using the term "further comprising" would, in most instances, be redundant.

Additionally, claims 20 and 22-25 were rejected under §112, second paragraph as being indefinite.

With regard to claim 20, the Examiner stated it is not clear how it is possible to store a program in read-only memory. The basis for this rejection is not entirely clear since it is always necessary, at some point, to store a program, or other data, in a read-only memory, in the sense of entering the program or the data into that memory. Even though after the storage takes place, the only action that can be

taken is to read information out of the memory, this does not make the phrase "storing a program in a read-only memory" indefinite or unclear. Nevertheless, there is not particular reason why the memory in the claims of the present application must necessarily be a read-only memory, and therefore that modifier has been removed from the claims of the present application.

Applicant also notes that the Examiner had no difficulty in citing a passage in the "keytool" reference that, according to the Examiner, teaches storing cryptographic algorithms in a read-only memory.

In claims 20, 23, 24 and 25, the various phrases beginning "upon a need for..." were stated to be unclear, and each of those claims has been editorially amended in a manner closely corresponding to the manner suggested by the Examiner.

With regard to claim 22, the Examiner stated it is not clear how implementation programs are contained within the logic modules, because the Examiner stated it is his understanding that programs are typically composed of logic modules, rather than vice versa. Applicant acknowledges that programs are often composed of software modules, which may be considered as "logic modules," but Applicant submits that the term "logic module" does not necessarily have to be used or constrained in this manner. Applicants are using the term "logic module" in the present application, as is clear from the present specification, as corresponding to a "logic circuit." This is consistent with the use of the term "security module" in the specification and claims of the present application, which is a physical, plug-in device.

Since a patent applicant is permitted to be his or her own lexicographer, Applicant submits that the use of the term "logic modules" in the present claims is not objectionable, and is easily understandable by those of ordinary skill in the relevant technology.

A lack of antecedent basis was noted in claim 24, which has been corrected.

All claims of the application are therefore submitted to be in full compliance with all provisions of §112, second paragraph.

Claims 1, 20, 25 and 26 were rejected under 35 U.S.C. §103(a) as being unpatentable over Heiden et al. in view of the aforementioned "keytool" reference. This rejection is respectfully traversed for the following reasons.

In substantiating the aforementioned rejection, the Examiner stated the Heiden et al. reference discloses securing a communication for a first purpose using a first signature, securing a communication for a second purpose using a second signature, and using a cryptographic algorithm of a first type to generate the first signature and using a cryptographic algorithm of a second type to generate the second signature.

The Examiner acknowledged that the Heiden et al. reference does not disclose that the cryptographic algorithms of the first and second types, for a same input set, respectively generate different outputs. The Examiner relied on the "keytool" reference as, according to the Examiner, teaching cryptographic algorithms of a first type and a second type and, for a same input set, respectively generating different respective outputs. The Examiner cited the RSA and DSA signatures described at page 4 of the "keytool" reference for this purpose.

Applicant respectfully submits the Examiner has read much more into the "keytool" reference than would be the case for a person of ordinary skill in the field of cryptographically securing communications who has not had the benefit of first reading the Applicant's disclosure. Applicant submits that the "keytool" reference merely describes a library or repository for different types of signatures, two examples of which, as noted by the Examiner, are an RSA signature and a DSA signature. As clearly stated at page 4 of the "keytool" reference, however, the algorithm that is used is strictly dependent on the type of key that is intended to be used, and therefore different keys result in the use of different algorithms, and thus result in the output of different signatures.

The Heiden et al. reference does disclose the use of different cryptographic algorithms respectively for different types of communications, however, those different algorithms operate on *different* inputs, corresponding to the different types of communications that are intended. By contrast, in the subject matter of the present application, the same input is supplied to the first computer and the only difference is that this input is accompanied by a designation as to which communication purpose is intended for a current communication. Dependent on the designated purpose of the communication, the appropriate one of the two available cryptographic algorithms is selected, plus also meaning that one of the two signature possibilities is then employed. As stated in the original language of the claim, however, the algorithms, and thus the signatures, act on the same input. This is summarized in the paragraph bridging pages 3 and 4 of the specification.

Therefore, even if the Heiden et al. reference were provided with a library or signature repository of the type disclosed in the "keytool" reference, this would not go beyond the teachings that are already present in the Heiden et al. disclosure. The different signatures available in the "keytool" library would simply be access for the different types of communication that are disclosed in the Heiden et al. reference, but in the Heiden et al. reference it is the input set for the particular communication, which will be the current communication that determines or causes a particular algorithm to be employed. If it were desired to use the same input set for either type of communication, with the only difference then being which type of signature were employed dependent on which type of communication purpose is intended, it is not even clear that the Heiden et al. system could function. In the Heiden et al. system, it is necessary that two different input sets be used for the respective different types of communication purposes, and it is because two different input sets are used that the Heiden et al. reference then "knows" which type of encryption algorithm to employ.

Independent claim 1 has been amended consistent with the above discussion and for the reasons discussed above Applicant submits that none of claims 1, 20, 25 and 26 would have been obvious to a person of ordinary skill in the field of cryptographically securing communications, under the provisions of 35 U.S.C. §103(a), based on the teachings of Heiden et al. and the "keytool" reference.

Claims 21-24 were rejected under 35 U.S.C. §103(a) as being unpatentable over the Heiden et al. and "keytool" references, further in view of the Examiner taking official notice of certain items in claims 21-24. Applicant submits that the above discussion is applicable to this rejection as well. Even if the items for which the

Examiner has taken "official notice" are known in the art, modifying the Heiden et al./"keytool" combination in accordance with that known information still would not result in the subject of any of claims 21-24.

All claims of the application are therefore submitted to be in condition for allowance.

It is expected that the Examiner would consider the changes in the claims that are made herein to raise a "new issue" such that the present Amendment would not have been entered if filed following the Final Rejection. Therefore, the present Amendment is being filed simultaneously with an RCE, and entry and consideration of the Amendment are respectfully requested.

The Commissioner is hereby authorized to charge any additional fees which may be required, or to credit any overpayment to account No. 501519.

Submitted by,

Steven N. Nowl (Reg. 28,982)

SCHIFF, HARDIN LLP
CUSTOMER NO. 26574
Patent Department
6600 Sears Tower
233 South Wacker Drive
Chicago, Illinois 60606
Telephone: 312/258-5790
Attorneys for Applicant.

CH1\ 6048775.1